

REMARKS

The foregoing remarks are responsive to the Final Office Action mailed June 17, 2004. Applicant respectfully requests reconsideration of the present application.

Claims 1-31 are pending. No claims have been amended, cancelled, withdrawn or added. Therefore, claims 1-31 are presented for examination.

Examiner rejected claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. Examiner rejected claims 2-4 and 20-22 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,233,685 issued to Smith, et al. Examiner rejected claims 7, 10, 25 and 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,581,161 issued to Byford. Examiner rejected claims 15, 16, 18 and 21 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 5,692,106 issued to Towers, et al. Examiner rejected claims 19 and 22 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,151,676 issued to Cuccia, et al. and further in view of U.S. Patent No. 6,119,227 issued to Mao.

Cuccia discusses a public key cryptosystem employing El-Gamal algorithm. The portion reference by the Examiner, column 6, lines 13-49 discuss how passphrase or biometric data is used to generate a user identifying key, which is then used to encrypt the user's private key. However, the passphrase or biometric information is immediately deleted from the system once the private key is encrypted. (Cuccia, column 7, lines 13-15):

In contrast, claim 1 recites in part:

receiving a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the server;
receiving the user's authentication data from the client;

determining if the user's authentication data matches the record ID; and Cuccia does not teach or suggest using a record ID for authentication within a public key system. In fact, Cuccia does not use a record ID because the user's authentication information is deleted immediately after it is used to generate a user identifying key. Therefore, Cuccia does not teach or suggest "determining if the user's authentication data matches the record ID" as recited in claim 1. Hence, Cuccia does, not anticipate claim 1, and claims 2-13, which depend on it.

Similarly, claim 14 recites in part:

looking up a record ID associated with the user;
generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

As discussed above with respect to claim 1, Cuccia does not teach or suggest looking up a record ID associated with the user. Therefore, claim 14, and claims 15-16 which depend on it, are not anticipated by Cuccia.

Claim 17 recites in part:

an authentication server to receive a record ID for a user, and a one-time key generated by a third party server and encrypted with a user's public key by the third party server;

a comparison logic in the authentication server to receive user authentication data from the client and determine whether the user's authentication data matches the record ID; and

As noted above, Cuccia does not teach or suggest a record ID for a user, being involved in the authentication process. Therefore, claim 17, and claims 18-31 which depend on it, are not anticipated by Cuccia.

Examiner rejected claims 2-4 and 20-22 under 35 U.S.C. §103(a) as being unpatentable over Cuccia and further in view of Smith. Claims 2-4 and 20-22 depend on claims 1 and 17, and incorporate its limitations. As discussed above, Cuccia discusses a public key cryptosystem employing El-Gamal algorithm, which employs user identifying keys determined by hashing the user's respective passphrases or

biometric information. Smith teaches a method and apparatus for establishing the provable integrity of a device. Smith does not teach or suggest using a record ID for authentication within a public key system. Therefore, Smith does not cure the shortcomings of Cuccia. Thus claims 2-4 and 20-22 are not obvious over Cuccia in view of Smith.

Examiner rejected claims 7, 10, 25 and 28 under U.S.C. §103(a) as being unpatentable over Cuccia in view of Byford. Byford discusses the use of a portable communication device (i.e. smart card) and providing controlled access to a facility. Byford does not teach or suggest using a record ID for authentication within a public key system. Therefore, Byford does not overcome the shortcomings of Cuccia. Thus, claims 7, 10, 25 and 28 are not obvious over Cuccia in view of Byford.

Examiner rejected claims 15, 16, 18 and 21 under 35 U.S.C. §103(a) as being unpatentable over Cuccia in view of Towers. Towers discusses fault diagnosis and service installation systems in a computer system, using an inference engine. However, Towers does not teach or suggest using a record ID for authentication within a public key system. Therefore, Towers does not cure the shortcomings of Cuccia. Thus, claims 15, 16, 18 and 21 are not obvious over Cuccia in view of Towers.

Examiner rejected claims 19 and 22 under 35 U.S.C. §103(a) as being unpatentable over Cuccia in view of Mao. Mao discusses authentication by an intermediary. However, Mao does not teach or suggest using a record ID for authentication within a public key system. Therefore, Mao does not cure the shortcomings of Cuccia. Thus, claims 19 and 22 are not obvious over Cuccia in view of Mao.

In view of the foregoing remarks, Applicant respectfully submits that all pending claims are in condition for allowance. Such allowance is respectfully requested.

If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Judith A. Szepesi at (408) 720-8300.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

Date: 8/17/04


Judith A. Szepesi
Reg. No. 39,393

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300